UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/774,285	01/30/2001	Young Sook Lim	KT-2 (KTP/0/2101)	2529

7265 7590 06/04/2004

MICHAELSON AND WALLACE
PARKWAY 109 OFFICE CENTER
328 NEWMAN SPRINGS RD
P O BOX 8489
RED BANK, NJ 07701

EXAMINER	
DADA, BEEMNET W	
ART UNIT	PAPER NUMBER
2135	6

DATE MAILED: 06/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/774,285	**Applicant(s)** LIM ET AL.	
	Examiner Beemnet W Dada	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

1. Claims 1-6 have been examined.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-6 have been rejected under 35 U.S.C 103(a) as being unpatentable over Adams et al. (hereinafter Adams) (Ref U).

4. As per claim 1, Adams teaches a method of providing a time stamping service for setting a client's system clock, comprising the steps of:

a) requesting the time stamping service of a time stamp authority server by a service requester [page 1, abstract and page 3, section 2.2, first paragraph];

b) receiving the time stamping service request from said requester and creating and sending a response message corresponding thereto by said time stamp authority server [page 3, section 2.2, 1st and 2nd paragraphs];

c) receiving the response message sent from said time stamp authority server and verifying the integrity thereof by said requester [page 3, section 2.2, 2nd paragraph];

d and e) downloading a certificate revocation list from a directory server and verifying the validity thereof by said requester, and downloading a certificate for an electronic signature of said time stamp authority server from said directory server, verifying an electronic signature value thereof [page 3, section 2.2, 3rd paragraph and page 16 and 17, Appendix B]. However, Adams does not explicitly teach setting the client's system clock in accordance with the verified result by said requester. It would have been obvious to one having ordinary skill in the art at the time the invention was made to set client's system clock in accordance with the verified result by said requester. It would have been obvious because Adams teaches receiving (i.e., by the client) a time stamping service from a TSA and verifying the validity of the TSA. Based on this teaching it would have been obvious to one having ordinary skill in the art to set client's system clock in accordance with the verified result.

5. As per claim 2, Adams teaches the method as applied to claim 1 above. Furthermore, Adams teaches the method wherein said step a) includes the steps of:

a-1) generating a random number with a given value and setting it as a nonce value of a service request message (TimeStampReq) [page 4, section 2.4.1 and page 5, paragraph 1];

a-2) use of extension field for additional information [page 4th paragraph];

a-3), and filling other parameters of said TimeStampReq message with given values and sending the resulting TimeStampReq message to said time stamp authority server [page 4, section 2.4.1].

6. As per claim 3, Adams teaches the method as applied to claim 1 above. Furthermore, Adams teaches the method wherein said step b) includes the steps of:

b-1) receiving a service request message (TimeStampReq) sent from said requester and authenticating and verifying the received TimeStampReq message [page 3, section 2.2, 1st and 2nd paragraphs];

b-2) if there is an error at said step b-1), processing the received TimeStampReq message as an erroneous message, sending the processed result to said requester and ending the corresponding process [page 6];

b-3) if there is no error at said step b-1), filling parameters of the response message (TimeStampResp) with given values [page 7];

b-4) and b-5) extracting a TSTInfo structure from a TimeStampResp message ;structure created at said b-3) and, in turn, current time information (a genTime value) from the extracted TSTInfo structure [page 7], calculating a message authentication code (MAC) value on the basis of the extracted genTime value and a nonce value, set by said requester and contained in said TimeStampReq message, and setting the calculated MAC value and identifier information of an algorithm used for the calculation of the MAC value respectively in corresponding fields of a MacInfo structure to assure the integrity of said response message [page 7 and page 8, 1st paragraph], adding the resulting MacInfo structure to an extension field of said TSTInfo structure and thus completing the creation of said TimeStampResp message structure [page 7 and page 8, 1st paragraph]; and

b-6) sending the completed response message (TimeStampResp) to said requester [page 3, section 2.2, 1st paragraph].

7. As per claim 4, Adams teaches the method as applied to claim 1 above. Furthermore, Adams teaches the method, wherein said step c) includes the steps of:

c-1) receiving the response message (TimeStampResp) sent from said time stamp authority server and authenticating and verifying the received response message [page 3, section 2.2, 2nd paragraph];

c-2) extracting a TSTInfo structure from said TimeStampResp message and, in turn, current time information (a genTime value) from the extracted TSTInfo structure, finding a nonce value, set by said requester and sent to said time stamp authority server, and directly calculating a message authentication code (MAC) value on the basis of the extracted genTime value and the found nonce value to check the integrity of said TimeStampResp message [page 7];

c-3) extracting a MacInfo structure from said TimeStampResp message sent from said time stamp authority server and, in turn, a MAC value from the extracted MacInfo structure and comparing the extracted MAC value with said MAC value calculated at said step c-2) to determine whether the two MAC values are equal [page 7 and page 8, 1st paragraph, and

c-4) if said two MAC values are not equal, recognizing that the current time information (genTimevalue) sent from said time stamp authority server was altered during the sending and said client's system clock cannot thus be set and then processing the received response message as an erroneous message, and if said two MAC values are equal, recognizing that the integrity of the received response message has been assured [page 7 and page 8, 1st paragraph].

8. As per claims 5 and 6, Adams teaches the method as applied to claim 1 above. Furthermore, Adams teaches verifying the Time Server Authority's certificate validity using Certificate Revocation List [page 3, section 2.2, paragraph 3, and pages 16 and 17].

9. Claims 1-6 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Sites (US Patent No. 6,728,880 B1) in view of Moses et al. (hereinafter refereed to as Moses) (US Patent No. 6,314,517 B1).

10. As per claim 1, Sites teaches a method of providing a time stamping service for setting a client's system clock, comprising the steps of:

a) requesting the time stamping service of a time stamp authority server by a service requester [column 2, lines 12-19, figure 1, step 110];

b) receiving the time stamping service request from said requester and creating and sending a response message corresponding thereto by said time stamp authority server [column 2, lines 12-25, figure 1, step 120];

c) receiving the response message sent from said time stamp authority server and verifying the integrity thereof by said requester [column 2, lines 26-54];

d and e) Furthermore, Sites teaches validating the sending server using digital signatures, where the time data is encrypted with private key of the sending server and decrypted with public key of the server [column 2, lines 45-55], and setting the client's system clock in accordance with the verified result by said requester [column 2, lines 35-42 and lines 65-67]. However, Sites does not expressly teach verifying the validity by downloading a certificate revocation list from a directory.

Moses teaches a method of downloading a certificate revocation list from a directory server and verifying the validity of a certificate of an electronic signature of a sending unit thereof by a receiving unit [column 1, lines 22-62, column 3, lines 47-64]. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to verify the validity of a certificate of an electronic signature of a sending unit by downloading a certificate revocation list from a directory server as per teachings of Moses into public / private keys (digital signature) validation method thought by Sites in order to confirm the public / private keys are valid (the certificate has not been revoked).

11. As per claim 2, the combination of Sites and Moses teaches the method as applied to claim 1 above. Furthermore, Sites teaches the steps of sending a request to a time stamp service, where the request includes local time and a random counter value) [column 2, lines, 12-16, 26-39].

12. As per claims 3 and 4, the combination of Sites and Moses teaches the method as applied to claim 1 above. Furthermore, Sites teaches receiving a request for a trust time information from a requestor, including a local time value and a random counter value sent by the requestor [column 2, lines 27-42], and verifying the validity of the message using the counter value [column 2, lines 37-42].

13. As per claims 5 and 6, the combination of Sites and Moses teaches the method as applied to claim 1 above. Furthermore, Moses teaches Moses teaches a method of downloading a certificate revocation list from a directory server and verifying the validity of a certificate of an electronic signature of a sending unit thereof by a receiving unit [column 1, lines 22-62, column 3, lines 47-64].

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (703) 305-8895. The examiner can normally be reached on Monday - Friday (8:30 am - 6:00 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

May 19, 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100